UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/720,214	11/25/2003	Ming-Fong Yeh	P24609	4973

7055 7590 03/03/2009

GREENBLUM & BERNSTEIN, P.L.C.
1950 ROLAND CLARKE PLACE
RESTON, VA 20191

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
03/03/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

gbpatent@gbpatent.com
pto@gbpatent.com

Office Action Summary	Application No.	Applicant(s)	
	10/720,214	YEH ET AL.	
	Examiner	Art Unit	
	MATTHEW T. HENNING	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 February 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 June 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 2/10/2009.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/10/2009 has been entered.

Response to Arguments

Applicant's arguments filed 2/10/2009 have been fully considered but are moot in view of the new grounds of rejection presented below.

All objections and rejections not set forth below have been withdrawn.

Claims 1-39 have been examined.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim(s) 1-15 and 29-32 is/are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform

underlying subject matter, and therefore do not qualify as a statutory process. The encryption and decryption method including steps of inputting data, selecting an algorithm, encrypting the data, etc. is broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent. As such, the claims are rejected under 35 USC 101 as not falling within one of the four statutory categories of invention.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 7, 9, 11, and 29-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Marchant (US Patent Number 6,094,486).

Regarding claim 7, Marchant disclosed a data encryption method, the method comprising: constructing encryption definition data containing a plurality of encryption algorithm module indicators (See Marchant Col. 5 Lines 42-52); inputting digital data to be encrypted (See Marchant Col. 10 Lines 54-67); from the encryption definition data, selecting at random an encryption algorithm module indicator (See Marchant Col 10 Lines 54-67); with the selected encryption algorithm module indicator as a guide, controlling encryption processing of

the inputted digital data (See Marchant Col. 11 Lines 1-3), wherein the selected encryption algorithm module indicator dynamically maintains a balance between security level and processing speed (See Marchant Col. 11 Lines 1-3); but Marchant did not specifically disclose appending decryption information to the digital data that has undergone encryption processing for subsequent output, or wherein at least one of the plurality of encryption algorithm module indicators indicates an asymmetric encryption algorithm and at least one of the plurality of encryption algorithm module indicators indicates a symmetric encryption algorithm.

Marchant did, however, disclose sending decryption information with the digital data that has undergone encryption processing (Marchant Col. 11 Lines 30-40). It would have been obvious to the ordinary person skilled in the art at the time of invention to have "appended" the public code to the encrypted information for transmission. This would have been obvious because the ordinary person skilled in the art would have been motivated to transmit the data and its corresponding public code together for increased ease of correlation.

Further, Marchant disclosed that the encryption algorithms can be of any kind not requiring transmission of the key with the encrypted information (See Marchant Col. 5 Lines 50-65). Furthermore, both symmetric and asymmetric encryption algorithms were well known in the art at the time of invention. Therefore, it would have been obvious to the ordinary person skilled in the art at the time of invention to have included both types of algorithms in the set of selectable algorithms. This would have been obvious because the ordinary person skilled in the art would have been motivated to increase the amount of algorithms to choose from.

Regarding claim 11, Marchant disclosed a data encryption method, the method comprising the: constructing an encryption module database for storing a plurality of entries of

records of data, each of the entries of records containing an encryption algorithm module indicator and an authentication algorithm module indicator (See Marchant Col. 5 Lines 42-52); constructing encryption definition data which includes a plurality of encryption module database indexes (See Marchant Col. 5 Lines 42-52); inputting digital data to be encrypted (See Marchant Col. 10 Lines 54-67); from the encryption definition data, selecting at random an encryption module database index (See Marchant Col. 10 Lines 54-67); according to the retrieved encryption module database index, selecting an entry of record from the encryption module database (See Marchant Col. 10 Lines 54-67); with the selected entry of record as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data (See Marchant Col. 11 Lines 1-3), wherein the selected encryption algorithm module indicator dynamically maintains a balance between security level and processing speed (See Marchant Col. 11 Lines 1-3); but Marchant failed to specifically disclose appending decryption information to the digital data that has undergone encryption for subsequent output (See Tan Col. 4 Lines 7-23), or wherein the encryption algorithm module indicator of one of the plurality of entries of records of data indicates an asymmetric encryption algorithm and the encryption algorithm module indicator of another of the plurality of entries of records of data indicates a symmetric encryption algorithm.

Marchant did, however, disclose sending decryption information with the digital data that has undergone encryption processing (Marchant Col. 11 Lines 30-40). It would have been obvious to the ordinary person skilled in the art at the time of invention to have "appended" the public code to the encrypted information for transmission. This would have been obvious

because the ordinary person skilled in the art would have been motivated to transmit the data and its corresponding public code together for increased ease of correlation.

Further, Marchant disclosed that the encryption algorithms can be of any kind not requiring transmission of the key with the encrypted information (See Marchant Col. 5 Lines 50-65). Furthermore, both symmetric and asymmetric encryption algorithms were well known in the art at the time of invention. Therefore, it would have been obvious to the ordinary person skilled in the art at the time of invention to have included both types of algorithms in the set of selectable algorithms. This would have been obvious because the ordinary person skilled in the art would have been motivated to increase the amount of algorithms to choose from.

Regarding claim 29, Marchant disclosed a data decryption method, the method comprising: inputting digital data to be decrypted (See Marchant Col. 11 Lines 41-44); retrieving the decryption algorithm module indicator and, upon a negative determination, setting the data to be decrypted as equivalent to inputted data for subsequent processing (See Tan Col. 13 Lines 4-39 and Col. 8 Lines 3-6); with the retrieved decryption algorithm module indicator as a guide, controlling decryption processing of the inputted digital data (See Tan Col. 13 Lines 4-39) , wherein the retrieved decryption algorithm module indicator dynamically maintains a balance between security level and processing speed (See Tan Col. 10 Lines 37-55); and outputting the digital data that has undergone decryption (See Tan Col. 13 Lines 4-39), but Marchant failed to specifically disclose inspecting to determine whether the digital data includes a decryption algorithm module indicator and, upon an affirmative determination, performing the decryption operations, and upon the negative determination outputting the data without

decrypting it; or that the decryption algorithm was retrieved from a decryption module database which stores a plurality of decryption algorithm module indicators, with at least one of the plurality of decryption algorithm module indicators indicating an asymmetric decryption algorithm and at least one of the plurality of decryption algorithm module indicators indicating a symmetric decryption algorithm.

Marchant did, however, disclose sending decryption information with the digital data that has undergone encryption processing (Marchant Col. 11 Lines 30-40). It would have been obvious to the ordinary person skilled in the art at the time of invention to have "appended" the public code to the encrypted information for transmission. This would have been obvious because the ordinary person skilled in the art would have been motivated to transmit the data and its corresponding public code together for increased ease of correlation. It further would have been obvious to the ordinary person skilled in the art to not append encryption information to the data if it is not encrypted, and upon receipt of data without encryption information to not attempt to decrypt the data. This would have been obvious because the ordinary person skilled in the art would have been motivated to avoid unnecessary computation and transmission of unnecessary data.

Further, Marchant disclosed that the encryption algorithms can be of any kind not requiring transmission of the key with the encrypted information (See Marchant Col. 5 Lines 50-65). Furthermore, both symmetric and asymmetric encryption algorithms were well known in the art at the time of invention. Therefore, it would have been obvious to the ordinary person skilled in the art at the time of invention to have included both types of algorithms in the set of

selectable algorithms. This would have been obvious because the ordinary person skilled in the art would have been motivated to increase the amount of algorithms to choose from.

Regarding claim 31, Marchant disclosed a data decryption method, the method comprising: constructing a decryption module database for storing a plurality of entries of records of data, each of the plurality of entries of records of data being a decryption algorithm module indicator (See Marchant Col. 5 Lines 42-52); inputting digital data to be decrypted (See Marchant Col. 10 Lines 54-67); retrieving the decryption module database index (See Marchant Col. 10 Lines 54-67); with the retrieved decryption module database index as a guide, selecting an entry of record from the decryption module database (See Marchant Col. 10 Lines 54-67); with the selected entry of record as a guide, controlling decryption processing of the inputted digital data (See Marchant Col. 11 Lines 1-3), wherein the retrieved decryption algorithm module indicator dynamically maintains a balance between security level and processing speed (See Marchant Col. 11 Lines 1-3); and outputting the digital data that has undergone decryption (See Marchant Col. 11 Lines 1-3), but Marchant failed to specifically disclose that one of the plurality of entries of records of data being a decryption algorithm module indicator indicates an asymmetric decryption algorithm and another of the plurality of entries of records of data being a decryption algorithm module indicators indicates a symmetric decryption algorithm; or inspecting to determine whether the digital data includes a decryption module database index and, upon an affirmative determination, performing the decryption processing, and upon the negative determination outputting the data without decrypting it.

Marchant did, however, disclose sending decryption information with the digital data that has undergone encryption processing (Marchant Col. 11 Lines 30-40). It would have been obvious to the ordinary person skilled in the art at the time of invention to have "appended" the public code to the encrypted information for transmission. This would have been obvious because the ordinary person skilled in the art would have been motivated to transmit the data and its corresponding public code together for increased ease of correlation. It further would have been obvious to the ordinary person skilled in the art to not append encryption information to the data if it is not encrypted, and upon receipt of data without encryption information to not attempt to decrypt the data. This would have been obvious because the ordinary person skilled in the art would have been motivated to avoid unnecessary computation and transmission of unnecessary data.

Further, Marchant disclosed that the encryption algorithms can be of any kind not requiring transmission of the key with the encrypted information (See Marchant Col. 5 Lines 50-65). Furthermore, both symmetric and asymmetric encryption algorithms were well known in the art at the time of invention. Therefore, it would have been obvious to the ordinary person skilled in the art at the time of invention to have included both types of algorithms in the set of selectable algorithms. This would have been obvious because the ordinary person skilled in the art would have been motivated to increase the amount of algorithms to choose from.

Regarding claim 33, Marchant disclosed a data decryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after decryption processing thereof (See Marchant Col. 5 Lines 42-52), the apparatus further comprising: retrieving the decryption algorithm module indicator (See Marchant Col. 10 Lines 54-67); and a

decryption processing portion for controlling decryption processing of the inputted digital data using the decryption algorithm module indicator retrieved by the inspecting portion as a guide (See Marchant Col. 10 Lines 54-67), wherein the retrieved decryption algorithm module indicator dynamically maintains a balance between security level and processing speed (See Marchant Col. 10 Lines 54-67), but Marchant failed to specifically disclose an inspecting portion for inspecting whether the data inputted via the input portion includes a decryption algorithm module indicator and, upon an affirmative inspection result, the apparatus decrypting the data, or, upon a negative inspection result, transmitting the inputted data directly to the output portion; or that the decryption module database which stores a plurality of decryption algorithm module indicators, with at least one of the plurality of decryption algorithm module indicators indicating an asymmetric decryption algorithm and at least one of the plurality of decryption algorithm module indicators indicating a symmetric decryption algorithm.

Marchant did, however, disclose sending decryption information with the digital data that has undergone encryption processing (Marchant Col. 11 Lines 30-40). It would have been obvious to the ordinary person skilled in the art at the time of invention to have "appended" the public code to the encrypted information for transmission. This would have been obvious because the ordinary person skilled in the art would have been motivated to transmit the data and its corresponding public code together for increased ease of correlation. It further would have been obvious to the ordinary person skilled in the art to not append encryption information to the data if it is not encrypted, and upon receipt of data without encryption information to not attempt to decrypt the data. This would have been obvious because the ordinary person skilled in the art

would have been motivated to avoid unnecessary computation and transmission of unnecessary data.

Further, Marchant disclosed that the encryption algorithms can be of any kind not requiring transmission of the key with the encrypted information (See Marchant Col. 5 Lines 50-65). Furthermore, both symmetric and asymmetric encryption algorithms were well known in the art at the time of invention. Therefore, it would have been obvious to the ordinary person skilled in the art at the time of invention to have included both types of algorithms in the set of selectable algorithms. This would have been obvious because the ordinary person skilled in the art would have been motivated to increase the amount of algorithms to choose from.

Regarding claim 9, Marchant disclosed that the constructed encryption definition data includes a plurality of encryption algorithm module combinations, each of the encryption algorithm module combinations including an encryption algorithm module indicator and an authentication algorithm module indicator, an encryption algorithm module combination being selected at random from the retrieved encryption definition data, the selected encryption algorithm module combination being used as a guide for controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data (See Marchant Col. 10 Lines 54-67).

Regarding claims 30, 32, and 34, Marchant disclosed that the inspecting portion inspects whether the data inputted via the input portion includes a decryption algorithm module combination, the decryption algorithm module combination including a decryption algorithm module indicator and an authentication algorithm module indicator, and, upon an affirmative

determination, retrieves the decryption algorithm module combination or, upon a negative determination, transmitting directly the inputted data to the output portion, the decryption processing portion controlling the decryption processing, including the type of decryption and the type of authentication, of the inputted digital data using the decryption algorithm module indicator retrieved by the inspecting portion as a guide (See Marchant Col. 10 Lines 54-67).

Regarding claim 35, Marchant disclosed a decryption module database for storing a plurality of entries of records of data, each of the entries of records containing a decryption algorithm module indicator, the inspecting portion inspecting whether the data inputted via the input portion includes a decryption module database index and, upon an affirmative inspection result, retrieving the decryption module database index and further retrieving an entry of record from the decryption module database using the index and, upon a negative inspection result, directly transmitting the inputted data to the output portion, the decryption processing portion controlling the decryption processing of the inputted digital data using the entry of record retrieved by the inspecting portion as a guide (See the rejection of claim 33 above).

Regarding claim 36, Marchant disclosed that the decryption module database stores a plurality of entries of records of data, each of the entries of records containing a decryption algorithm module indicator and an authentication algorithm module indicator, the decryption processing portion controlling decryption processing, including the type of decryption and the type of authentication, using the entry of record retrieved by the inspecting portion as a guide (See Marchant Col. 10 Lines 54-67).

Claims 1, 3, 5, 13-16, 18, 20, 22, 23, 25, 27, 28, and 37-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Marchant, and further in view of Tan (US Patent Number 6,490,353).

Regarding claim 1, Tan disclosed a data encryption method, the method comprising: constructing a security class database for storing a plurality of entries of records of data (See Marchant Col. 5 Lines 42-52), each of the entries of records including a corresponding encryption definition field, the encryption definition field including a plurality of encryption algorithm module indicators, wherein at least one of the plurality of encryption algorithm module indicators indicates an asymmetric encryption algorithm and at least one of the plurality of encryption algorithm module indicators indicates a symmetric encryption algorithm (See Marchant Col. 5 Lines 42-52, and the rejection of claim 9 above); inputting digital data to be encrypted (See Marchant Col. 10 Lines 54-67); from the security class database, retrieving the corresponding encryption definition data (See Marchant Col. 10 Lines 54-67); from the retrieved encryption definition data, selecting at random an encryption value related to an algorithm module indicator (See Marchant Col. 10 Lines 54-67); with the selected encryption algorithm module indicator as a guide, controlling encryption processing of the inputted digital data (See Marchant Col. 11 Lines 1-3), wherein the selected encryption algorithm module indicator dynamically maintains a balance between security level and processing speed (See Marchant Col. 11 Lines 1-3); and appending decryption information to the digital data that has undergone encryption processing for subsequent output (See the rejection of claim 9 above), but Marchant failed to teach each record also including a data attribute description field; or finding a data attribute description that matches attribute of the digital data.

Tan teaches that that in a random encryption algorithm selection system the choice of complexity of the algorithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the algorithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Tan in the encryption system of Marchant by including an indication of the complexity level of each algorithm in the set and depending on the security and sensitivity level of the data being transmitted, choosing from the algorithms that meet that sensitivity level. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each algorithm and determining which algorithms were complex enough for the policy regarding the data being encrypted.

Regarding claim 5, Marchant disclosed a data encryption method, the method comprising: constructing an encryption module database for storing a plurality of entries of records of data, each of the plurality of entries of records of data containing an encryption algorithm module indicator and an authentication algorithm module indicator, wherein the encryption algorithm module indicator of one of the plurality of entries of records of data indicates an asymmetric encryption algorithm and the encryption algorithm module indicator of another of the plurality of entries of records of data indicates a symmetric encryption algorithm (See Marchant Col. 5 Lines 42-52 and the rejection of claim 9 above); inputting digital data to be encrypted (See Marchant Col. 10 Lines 54-67); finding each data attribute description that

matches an attribute of the digital data, and retrieving the corresponding encryption definition field (See Marchant Col. 10 Lines 54-67); from the retrieved encryption definition field, selecting at random an encryption module database indexes (See Marchant Col. 10 Lines 54-67); according to the retrieved encryption module database index, selecting an entry of record from the encryption module database (See Marchant Col. 10 Lines 54-67); with the selected entry of record as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data (See Marchant Col. 11 Lines 1-3), wherein the selected encryption algorithm module indicator dynamically maintains a balance between security level and processing speed (See Marchant Col. 11 Lines 1-3); and appending decryption information to the digital data that has undergone encryption processing for subsequent output (See the rejection of claim 9 above), but Marchant failed to disclose constructing a security class database for storing a plurality of entries of records of data, each of the entries of records containing a data attribute description field and a corresponding encryption definition field, the encryption definition field including a plurality of encryption module database indexes.

Tan teaches that that in a random encryption algorithm selection system the choice of complexity of the algorithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the algorithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Tan in the encryption system of Marchant by including an indication of the complexity level of each algorithm in the set and depending on the security and

sensitivity level of the data being transmitted, choosing from the algorithms that meet that sensitivity level. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each algorithm and determining which algorithms were complex enough for the policy regarding the data being encrypted.

Regarding claim 13, Marchant disclosed a data encryption method, the method comprising : constructing a security class database for storing a plurality of entries of records of data, each of the plurality of entries of records of data containing a corresponding encryption definition field, the encryption definition data field being an encryption algorithm module indicator, wherein the encryption algorithm module indicator of one of the plurality of entries of records of data indicates an asymmetric encryption algorithm and the encryption algorithm module indicator of another of the plurality of entries of records of data indicates a symmetric encryption algorithm (See Marchant Col. 5 Lines 42-52 and the rejection of claim 9 above); inputting digital data to be encrypted (See Marchant Col. 10 Lines 54-67); retrieving the encryption algorithm module indicator of the corresponding encryption definition field (See Marchant Col. 10 Lines 54-67); with the selected encryption algorithm module indicator as a guide, controlling encryption processing of the inputted digital data (See Marchant Col. 11 Lines 1-3), wherein the selected encryption algorithm module indicator dynamically maintains a balance between security level and processing speed (See Marchant Col. 10 Lines 54-67); and appending decryption information to the digital data that has undergone encryption processing for subsequent output (See the rejection of claim 9 above), but Marchant failed to disclose each

of the entries of records containing a data attribute description field; or from the security class database, finding each data attribute description that matches an attribute of the digital data.

Tan teaches that that in a random encryption algorithm selection system the choice of complexity of the algorithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the algorithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Tan in the encryption system of Marchant by including an indication of the complexity level of each algorithm in the set and depending on the security and sensitivity level of the data being transmitted, choosing from the algorithms that meet that sensitivity level. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each algorithm and determining which algorithms were complex enough for the policy regarding the data being encrypted.

Regarding claim 15, Marchant disclosed a data encryption method, the method including: constructing an encryption module database for storing a plurality of entries of records of data, each of the plurality of entries of records of data containing an encryption algorithm module indicator and an authentication algorithm module indicator, wherein the encryption algorithm module indicator of one of the first plurality of entries of records of data indicates an asymmetric encryption algorithm and the encryption algorithm module indicator of another of the first

plurality of entries of records of data indicates a symmetric encryption algorithm (See Marchant Col. 5 Lines 42-52 and the rejection of claim 9 above); inputting digital data to be encrypted (See Marchant Col. 10 Lines 54-67); retrieving the encryption module database index from the corresponding encryption definition field (See Marchant Col. 10 Lines 54-67); with the retrieved encryption module database index as a guide, selecting an entry of record from the encryption module database (See Marchant Col. 11 Lines 1-3); with the selected entry of record as a guide, controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data (See Marchant Col. 11 Lines 1-3), wherein the selected encryption algorithm module indicator dynamically maintains a balance between security level and processing speed (See Marchant Col. 11 Lines 1-3); and appending decryption information to the digital data that has undergone encryption processing for subsequent output (See the rejection of claim 9 above) however, Marchant failed to disclose constructing a security class database for storing a plurality of entries of records of data, each of the entries of records containing a data attribute description field and a corresponding encryption definition field, the encryption definition data field being an encryption module database index; or from the security class database, finding each data attribute description that matches attribute an of the digital data, and retrieving the encryption module database index from the corresponding encryption definition field.

Tan teaches that that in a random encryption algorithm selection system the choice of complexity of the algorithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors

or policies, and that depending on the requirements of the application, users, or policy a library of the algorithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Tan in the encryption system of Marchant by including an indication of the complexity level of each algorithm in the set and depending on the security and sensitivity level of the data being transmitted, choosing from the algorithms that meet that sensitivity level. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each algorithm and determining which algorithms were complex enough for the policy regarding the data being encrypted.

Regarding claim 16, Tan disclosed a data encryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after encryption processing thereof, the apparatus further comprising: a security class database for storing a plurality of entries of records of data, a corresponding encryption definition field, the encryption definition field including a plurality of encryption algorithm module indicators, wherein at least one of the plurality of encryption algorithm module indicators indicates an asymmetric encryption algorithm and at least one of the plurality of encryption algorithm module indicators indicates a symmetric encryption algorithm (See Marchant Col. 5 Lines 42-52 and the rejection of claim 9 above); an attribute inspecting portion for finding from the security class database each data attribute description that matches an attribute of the digital data sent from the inspecting portion and for transmitting the corresponding encryption definition data to a encryption selecting portion (See Marchant Col. 10 Lines 54-67); the encryption selecting

portion, selecting at random an encryption algorithm module indicator from the retrieved encryption definition data (See Marchant Col. 10 Lines 54-67); and an encryption processing portion for controlling encryption processing of the inputted digital data using the encryption algorithm module indicator selected by the encryption selecting portion as a guide (See Marchant Col. 11 Lines 1-3), wherein the selected encryption algorithm module indicator dynamically maintains a balance between security level and processing speed (See Marchant Col. 11 Lines 1-3), but Marchant failed to specifically disclose each of the entries of records containing a data attribute description field; an inspecting portion for inspecting and separating the data inputted via the input portion into parameter data or digital data; a parameter processing portion for updating the security class database with the parameter data sent from the inspecting portion.

Tan teaches that that in a random encryption algorithm selection system the choice of complexity of the algorithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the algorithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Tan in the encryption system of Marchant by including an indication of the complexity level of each algorithm in the set and depending on the security and sensitivity level of the data being transmitted, choosing from the algorithms that meet that sensitivity level. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each

algorithm and determining which algorithms were complex enough for the policy regarding the data being encrypted.

Regarding claim 23, Marchant disclosed a data encryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after encryption processing thereof, the apparatus further comprising: a encryption module database for storing a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator, wherein the encryption algorithm module indicator of one of the plurality of entries of records of data indicates an asymmetric encryption algorithm and the encryption algorithm module indicator of another of the plurality of entries of records of data indicates a symmetric encryption algorithm (See Marchant Col. 5 Lines 42-52 and the rejection of claim 9 above); a encryption selecting portion for selecting at random an entry of record from the encryption module database (See Marchant Col. 10 Lines 54-67); and an encryption processing portion for controlling encryption processing of the inputted digital data using the entry of record selected by the encryption selecting portion as a guide (See Marchant Col. 11 Lines 1-3), wherein the selected encryption algorithm module indicator dynamically maintains a balance between security level and processing speed (See Marchant Col. 11 Lines 1-3), but Marchant failed to specifically disclosed an inspecting portion for inspecting and separating the data inputted via the input portion into parameter data or digital data; a parameter processing portion for updating the encryption module database using the parameter data from the inspecting portion.

Tan teaches that that in a random encryption algorithm selection system the choice of complexity of the algorithms might be determined by the user based on the security and

sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the algorithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Tan in the encryption system of Marchant by including an indication of the complexity level of each algorithm in the set and depending on the security and sensitivity level of the data being transmitted, choosing from the algorithms that meet that sensitivity level. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each algorithm and determining which algorithms were complex enough for the policy regarding the data being encrypted.

Regarding claim 27, Marchant disclosed a data encryption apparatus, the apparatus having an input portion for input of data and an output portion for output of data after encryption processing thereof, the apparatus further comprising: a security class database for storing a plurality of entries of records of data, each of the entries of records containing a corresponding encryption definition field, the encryption definition field being an encryption algorithm module indicator, wherein the encryption algorithm module indicator of one of the plurality of entries of records of data indicates an asymmetric encryption algorithm and the enc13rption algorithm module indicator of another of the plurality of entries of records of data indicates a symmetric encryption algorithm (See Marchant Col. 5 Lines 42-52); and the encryption processing portion for controlling encryption processing of the inputted digital data using the encryption algorithm module indicator selected as a guide (See Marchant Col. 11 Lines 1-3), wherein the selected

encryption algorithm module indicator dynamically maintains a balance between security level and processing speed (See Marchant Col. 11 Lines 1-3), but Marchant failed to specifically disclose a security class database for storing a plurality of entries of records of data, each of the entries of records containing a data attribute description field and an inspecting portion for inspecting and separating the data inputted via the input portion into parameter data or digital data; a parameter processing portion for updating the security class database with the parameter data from the inspecting portion; an attribute inspecting portion for finding from the security class database each data attribute description that matches an attribute of the digital data sent from the inspecting portion and for transmitting the corresponding encryption definition data to an encryption processing portion.

Tan teaches that that in a random encryption algorithm selection system the choice of complexity of the algorithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the algorithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Tan in the encryption system of Marchant by including an indication of the complexity level of each algorithm in the set and depending on the security and sensitivity level of the data being transmitted, choosing from the algorithms that meet that sensitivity level. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each

algorithm and determining which algorithms were complex enough for the policy regarding the data being encrypted.

Regarding claims 3, 14, 18, 25, and 28, Marchant and Tan disclosed that the encryption definition field in the security class database constructed in step A is an encryption algorithm module combination, the encryption algorithm module combination including an encryption algorithm module indicator and an authentication algorithm module indicator, data of an encryption algorithm module combination of the corresponding encryption definition field being retrieved in the step C of finding from the security class database the data attribute description that matches the attribute of the digital data, the selected encryption algorithm module combination being used in step D as a guide for controlling encryption processing, including the type of encryption and the type of authentication, of the inputted digital data (See Marchant Col. 5 Lines 42-52 and the rejection of claim 9 above).

Regarding claim 20, Marchant and Tan disclosed an encryption module database for storing a plurality of entries of records of data, each of the entries of records containing an encryption algorithm module indicator and an authentication algorithm module indicator (See Marchant Col. 5 Lines 42-52); the encryption definition field of the security class database including a plurality of encryption module database indexes (See Marchant Col. 5 Lines 42-52); the encryption selecting portion selecting at random an encryption module database index from the retrieved encryption definition data and, according to the retrieved encryption module database index, and selecting an entry of record from the encryption module database (See Marchant Col. 10 Lines 54-67); the encryption processing portion using the entry of record selected by the encryption selecting portion as a guide to control encryption processing,

including the type of encryption and the type of authentication, of the inputted digital data (See Marchant Col. 11 Lines 1-3), wherein the selected entry of record dynamically maintains a balance between security level and processing speed (See Marchant Col. 11 Lines 1-3).

Regarding claim 22, Marchant and Tan disclosed that the parameter processing portion updates the security class database and the encryption module database using the parameter data sent from the inspecting portion (See Tan Col. 8 Lines 15-25 and the rejection of claim 9 above).

Regarding claim 37, Marchant and Tan disclosed the claimed decryption system including inspecting whether the digital data includes a decryption module database index and, upon an affirmative inspection result, retrieving the decryption module database index and further retrieving an entry of record from the decryption module database using the index and, upon a negative inspection result, directly transmitting the inputted data to the output portion (See Tan Col. 8 Lines 3-25 and Col. 13 Lines 4-39) but failed to specifically disclose a parameter processing portion for updating the decryption module database using parameter data, the inspecting portion inspecting and separating the data inputted via the input portion into parameter data or digital data and, if the inputted data is parameter data, transmitting the same to the parameter processing portion and, if the inputted data is digital data. However, Marchant and Tan did disclose that the choice of complexity of the securithms might be determined by the user based on the security and sensitivity level of the data in part, or in whole, purpose of the communication, or other factors or policies, and that depending on the requirements of the application, users, or policy a library of the algorithms from the pool are arbitrarily selected (See Tan Col. 8 Lines 15-25).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have included an indication of the complexity level of each algorithm in the pool, and selecting the algorithm based upon an appropriate complexity level required for the input data. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow the system to easily identify the complexity of each algorithm when determining which algorithms were complex enough for the policy regarding the data being encrypted.

Regarding claim 38, Marchant and Tan disclosed the decryption module database stores a plurality of entries of records of data, each of the entries of records containing a decryption algorithm module indicator and an authentication algorithm module indicator, the decryption processing portion controlling decryption processing, including the type of decryption and the type of authentication, of the inputted digital data using the entry of record retrieved by the inspecting portion as a guide (See Marchant Col. 11 Line 41 – Col. 12 Line 61).

Claims 2, 4, 6, 8, 10, 12, 17, 19, 21, 24, 26, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Marchant and Tan as applied to claims 1, 5, 7, 11, 16, 23, and 27 above, and further in view of Kim et al. (US Patent Number 6,499,127) hereinafter referred to as Kim.

Marchant and Tan disclosed randomly selecting one algorithm from a set of algorithms randomly and that the encryption definition field in the security class database includes a plurality of encryption algorithm module indicators and corresponding proportions adopted thereby (See Tan Col. 8 Lines 15-25 and Col. 9 Lines 34-40 and the rejection of claim 9 above), but failed to specifically disclose an encryption algorithm module indicator being selected from the retrieved encryption definition data according to each of the encryption algorithm module

indicators and the corresponding proportions adopted thereby in cooperation with a random number generator and a MOD operation.

Alternatively, Kim teaches a method for selecting a number in a range randomly comprising determining the size of the range, generating a random number, and taking the random number modulo the size of the range (See Kim Col. 23 Paragraph 1).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Kim in the random algorithm system of Marchant and Tan by selecting the algorithm randomly from the seed by generating a random number and then taking the random number MOD the number of entries in the seed. This would have been obvious because the ordinary person skilled in the art would have been motivated to select the algorithm randomly as taught by Marchant.

Regarding claim 39, Marchant and Tan disclosed that the parameter processing portion updates the security class database and the encryption module database using the parameter data sent from the inspecting portion (See Tan Col. 8 Lines 15-25).

Conclusion

Claims 1-39 have been rejected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Examiner, Art Unit 2431